MICHAEL F. RAM (SBN 104805)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
Telephone: (415) 358-6913
Facsimile: (415) 358-6923
mram@ForThePeople.com

JOHN YANCHUNIS
(*Pro Hac Vice application forthcoming*)
PATRICK BARTHLE
(*Pro Hac Vice application forthcoming*)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 559-4908
Facsimile: (813) 222-4795
jyanchunis@ForThePeople.com
pbarthle@ForThePeople.com

Attorneys for Plaintiffs and the Putative Class

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

THOMAS SHRIVER, and JAMES LEE, On Behalf of Themselves and All Others Similarly Situated, Plaintiffs, v. PARTNERSHIP HEALTHPLAN OF CALIFORNIA. Defendant.	Case No.: **CLASS ACTION COMPLAINT FOR:** (1) Negligence (2) Breach of Implied Contract (3) Invasion of Privacy (4) Violations of the Confidentiality of Medical Information Act **Jury Trial Demanded on All Causes of Action So Triable**

Plaintiffs Thomas Shriver and James Lee ("Plaintiffs"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against Partnership HealthPlan of California ("PHC" or "Defendant"), and alleges, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information and protected health information ("PHI") that Defendant's enrollees entrusted to it, including, without limitation, name, Social Security number, date of birth, Driver's License number (if provided), Tribal ID number (if provided), medical record number, treatment, diagnosis, prescription and other medical information, health insurance information, member portal username and password, email address, and address maintained by PHC (collectively, "personally identifiable information" or "PII").[1]

2. Partnership HealthPlan of California is "a non-profit community based health care organization that contracts with the State to administer Medi-Cal benefits through local care providers to ensure Medi-Cal recipients have access to high-quality comprehensive cost-effective health care."[2]

3. Upon information and belief, on or about March 19, 2022, Defendant discovered that its internal administrative system was breached by a ransomware group known as Hive, which accessed, exfiltrated and/or published the PII of more than 854,913 individuals, including that of Plaintiffs and Class Members, (the "Data

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).

[2] http://www.partnershiphp.org/Pages/PHC.aspx (last visited June 10, 2022).

Breach").[3]

4. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII and PHI, Defendant assumed legal and equitable duties to those individuals.

5. The exposed PII and PHI of Plaintiffs and Class Members can now be sold on the dark web and, upon information and belief, may already have been posted for sale. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiffs and Class Members face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

6. This PII and PHI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiffs and Class Members.

7. Plaintiffs brings this action on behalf of all persons whose PII and PHI was compromised as a result of Defendant's failure to: (i) adequately protect the PII and PHI of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of its inadequate information security practices; and (iii) avoid sharing the PII and PHI of Plaintiffs and Class Members without adequate safeguards. Defendant's conduct amounts to negligence and violates federal and state statutes.

8. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the present, continuing, and certainly increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to

[3] *See Data Breach Notifications*, OFFICE OF THE MAINE ATT'Y GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/88f036a8-2e3b-4262-9da5-8a6073110c61.shtml (last visited June 22, 2022).

access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

9. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs' and Class Members' PII and PHI was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII and PHI of Plaintiffs and Class Members was accessed, exfiltrated, and/or published by unauthorized third party.[4]

10. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

11. Plaintiff Thomas Shriver is a citizen of California residing in Humboldt County, California.

12. Plaintiff James Lee is a citizen of California residing in Humboldt County, California.

13. Defendant Partnership HealthPlan of California is a California corporation with its principal place of business in Fairfield, California. Defendant is headquartered at 4665 Business Center Drive, Fairfield, California 94534.

14. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

[4]

15. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d), as the amount in controversy exceeds the sum of $5,000,000, exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members are citizens of a different state than Defendant.

17. Venue is proper in this District pursuant to 18 U.S.C. § 1965(a) and 28 U.S.C. § 1391(b)(2) because Defendant conducts its affairs in this District and a substantial part of the events giving rise to Plaintiffs' claims occurred in or emanated from this District.

18. This Court has personal jurisdiction over Defendant because its principal place of business is in California. Additionally, Defendant is subject to specific personal jurisdiction in this District because a substantial part of the events and conduct giving rise to Plaintiffs' and the Class's claims occurred in this District. Defendant Partnership HealthPlan of California is a California corporation with its principal place of business in Fairfield, California. Defendant is headquartered at 4665 Business Center Drive, Fairfield, California, 94534.

IV. FACTUAL ALLEGATIONS

Background

19. Partnership HealthPlan of California is "a non-profit community based health care organization that contracts with the State to administer Medi-Cal benefits through local care providers to ensure Medi-Cal recipients have access to high-quality comprehensive cost-effective health care."[5]

[5] http://www.partnershiphp.org/Pages/PHC.aspx (last visited June 10, 2022).

20. Defendant manages Medi-Cal beneficiaries who reside in various Northern California counties. PHC is organized as a health insuring organization under California law. Defendant maintains regional offices in this District.

21. Defendant operates a managed health care system designed provide health care delivery to individuals in California, including in Del Norte, Humboldt, Lake, Lassen, Marin, Mendocino, Modoc, Napa, Trinity, Shasta, Siskiyou, Solano, Sonoma, and Yolo Counties in Northern California. PHC claims to currently serve approximately 600,000 members.

22. Defendant's Notice of Privacy Practices ("Privacy Policy"), contained within its Member Handbook,[6] updated and effective November 8, 2017, describes how medical information about its enrollees may be used and disclosed and how enrollees can get access to this information. It states: "[a] statement describing PHC policies and procedures for preserving the confidentiality of medical records is available and will be furnished to you upon request."[7]

The Privacy Policy provides Patient Rights and Responsibilities, and also states that Defendant is required by law to:

> Partnership HealthPlan of California is required by law to provide you with adequate notice of the uses and disclosures of your protected health information that PHC may make, and of your rights and our legal duties and to notify you following a breach of your unsecured health information where your protected health information (PHI) is concerned.[8]

Further, the Privacy Policy lists situations under which PHC may disclose PHI and PII of its enrollees without written authorization – none of which are applicable

[6] Exhibit 2 (*Member Handbook*), at 92.
[7] *Id.*
[8] *Id.*

here.[9]

In addition, the Privacy Policy explicitly states:

> OTHER THAN WHAT IS STATED ABOVE, PHC WILL NOT DISCLOSE YOUR HEALTH INFORMATION OTHER THAN WITH YOUR WRITTEN AUTHORIZATION. IF YOU OR YOUR REPRESENTATIVE AUTHORIZES PHC TO USE OR DISCLOSE YOUR HEALTH INFORMATION, YOU MAY REVOKE THAT AUTHORIZATION IN WRITING AT ANY TIME.[10]

23. As a condition of receiving healthcare services from Defendant, Plaintiffs and Class Members were required to provide their PHI and PII to Defendant.

24. Defendant collected and stored some of Plaintiffs' and Class Members' most sensitive and confidential personal and medical information, including, without limitation, name, Social Security number, date of birth, Driver's License number (if provided), Tribal ID number (if provided), medical record number, treatment, diagnosis, prescription and other medical information, health insurance information, member portal username and password, email address, and address. This includes information that is static, does not change, and can be used to commit myriad financial crimes.

25. Plaintiffs and Class Members relied on this sophisticated Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII and PHI.

26. Defendant had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII and PHI from involuntary disclosure to third parties.

---

[9] *Id.*

[10] *Id.*, at 97.

The Data Breach

27. On or about March 19, 2022, PHC discovered unauthorized activity on its internal computer systems. Upon discovering this activity, PHC "immediately began an investigation with the assistance of cybersecurity specialists"[11] Defendant's investigation revealed that unauthorized party accessed and/or took certain information from PHC's network on or about March 19, 2022 (the "Data Breach").

28. Defendant began informing clinics that its systems were down on March 21, 2022; on or about that date, Defendant's website was replaced with the following message:

> "Partnership HealthPlan of California recently became aware of anomalous activity on certain computer systems within its network. We are working diligently with third-party forensic specialists to investigate this disruption, safely restore full functionality to affected systems, and determine whether any information may have been potentially accessible as a result of the situation."[12]

29. Nearly three months later, on or about May 23, 2022, Defendant posted its Website Notice, which states, in part:

> Partnership HealthPlan of California ("PHC") is writing to make you aware of an incident that may affect the security of some of your information. We take this incident seriously, and write to provide you with information about the incident, what we are doing in response, and the resources that are available to you to help better protect your personal information from possible misuse, should you feel it is appropriate to do so.
>
> ***What Happened?*** On March 19, 2022, PHC identified unusual activity on its network. In response, PHC

[11] Ex. 1.

[12] *Partnership Healthplan of California Data Breach*, THE PRESS DEMOCRAT, https://www.pressdemocrat.com/article/news/medi-cal-healthplan-website-and-computer-systems-down/ (last visited June 21, 2022).

immediately began an investigation with the assistance of cybersecurity specialists. We have evidence that an unauthorized party accessed or took certain information from PHC's network on or about March 19, 2022.

What information was involved? Based on the investigation into this incident, it was determined that the information involved may include your name, Social Security number, date of birth, Driver's License number (if provided), Tribal ID number (if provided), medical record number, treatment, diagnosis, prescription and other medical information, health insurance information, member portal username and password, email address, and address.

What We are Doing: PHC started a thorough process to identify what information was ***potentially*** contained within the impacted files, and to whom that information belonged. That process is ongoing. While ***we have not confirmed what specific information may have been accessed or taken, because the possibility exists***, we are now notifying those individuals whose information was potentially impacted by the incident. In addition, we notified federal law enforcement, with reference number I2203221559516532, and are notifying regulatory authorities as required by law. We are also notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so. In addition, we arranged to have Cyberscout, a TransUnion company, provide credit monitoring services for two years at no cost to you.

We regret that this incident occurred and want to assure you that we have taken many steps to increase existing security and are reviewing our existing policies and procedures to identify additional safeguards which may further secure the information in our systems.

> ***What You Can Do:*** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. You may also enroll in the complimentary credit monitoring services we are making available to you. Enrollment instructions are attached to this letter.[13]

30. Defendant admitted in the Website Notice that an unauthorized party actually or potentially compromised sensitive information about Plaintiffs and Class Members, including name, Social Security number, date of birth, Driver's License number (if provided), Tribal ID number (if provided), medical record number, treatment, diagnosis, prescription and other medical information, health insurance information, member portal username and password, email address, and address, information maintained by PHC.

31. On or about May 18, 2022, Defendant notified the Office of the Maine Attorney General of the Data Breach.[14] On or about May 18, 2022, Defendant notified the California Attorney General of the Data Breach. Defendant also provided the states Attorneys General with letters and/or "sample" notices of the Data Breach.[15]

32. On or about May 18, 2022, Defendant began to send Data Breach Notification Letters to Plaintiffs and Class Members.[16]

33. In response to the Data Breach, Defendant claims that it "implemented additional security measures to protect our digital environment and minimize the likelihood of future incidents."[17]

---

[13] Ex. 1 (emphasis added).
[14] *PHC Health Data Breach Notice to Consumers*, OFF. OF THE ME. ATT'Y GEN. (May 18, 2022), *available at* https://apps.web.maine.gov/online/aeviewer/ME/40/88f036a8-2e3b-4262-9da5-8a6073110c61.shtml.
[15] Exhibit 3 (Sample *Notice of Data Breach* provided to California Attorney General).
[16] https://apps.web.maine.gov/online/aeviewer/ME/40/88f036a8-2e3b-4262-9da5-8a6073110c61.shtml (last visited June 21, 2022).
[17] Ex. 2 at 1.

34. However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information is protected.

35. Further, Defendant has maintained secret the very nature of the Data Breach. As of June 22, 2022, Defendant has not yet confirmed the ransomware attack, nor has it indicated to its current and former enrollees, including Plaintiffs and Class Members, that their information was likely stolen and posted on the dark web.

The Hive Ransomware Attack

36. Contrary to Defendant's assertions, public reports began emerging on or about March 29, 2022, that the Data Breach was actually the result of a ransomware attack by the ransomware group known as the Hive ("Hive"). As early as March of 2022, information from the Data Breach was offered for sale on a dark web data leak website, "HiveLeaks."

37. On or about March 29, 2022, Hive placed a posting on its dark web ToR page called "HiveLeaks," alleging that it had stolen 850,000 unique records containing PII from Defendant's File Server and encrypted the same on PHC servers on March 19, 2022.

38. In its post, Hive claimed to have exfiltrated upwards of 850,000 unencrypted, personal, unique records from PHC's systems.[18] These records each contained, allegedly, PII and PHI, including "Name, Surname, SSN, DOB, Address, Contact, etc."[19] Hive also alleged it had stolen 400 Gigabytes of data from PHC file servers.

---

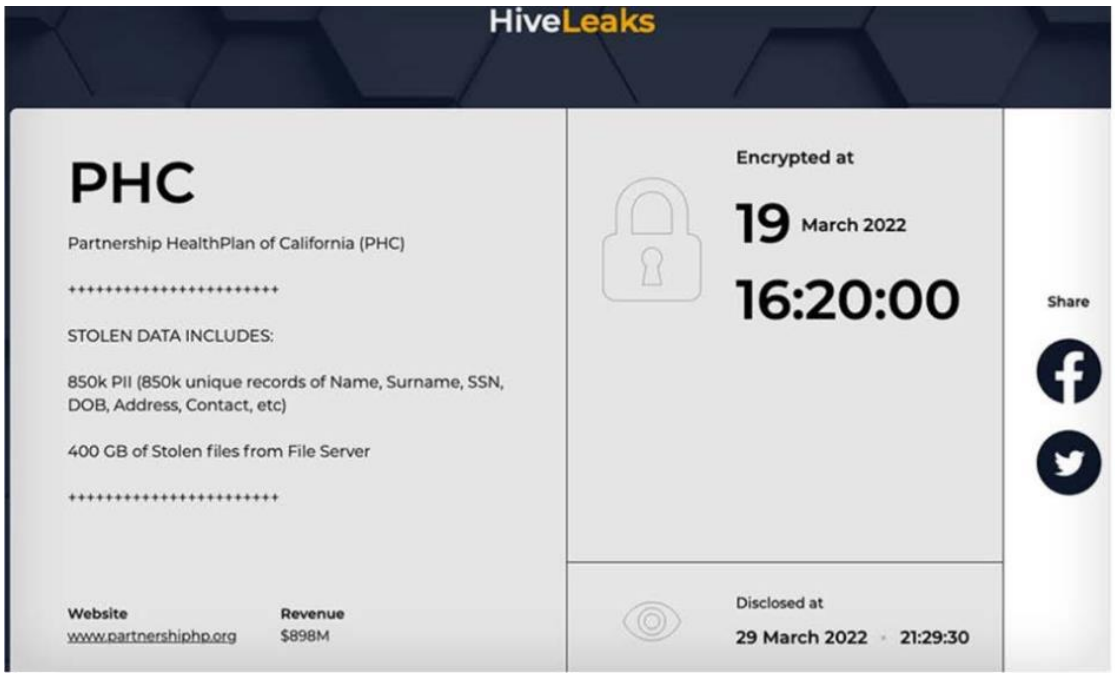
[18] April Strauss, Esq., *Partnership HealthPlan of California Possibly One of the Largest Healthcare Data Breaches in US*, LEGALSCOOPS (May 6, 2022, updated May 21, 2022), legalscoops.com/partnership-healthplan-of-california-data-breach-possibly-one-of-the-largest-in-health-care/ (last visited June 22, 2022).

[19] April Strauss, Esq., *Partnership HealthPlan of California Possibly One of the Largest Healthcare Data Breaches in US*, LEGALSCOOPS (May 6, 2022, updated May 21, 2022),

39. Defendant, in its sample Breach Notification Letters, stated numerous times that, while it had "evidence" that some information "may have been accessed or taken," the vague language fails to reveal the true nature of Defendant's knowledge of the incident.[20]

40. Upon information and belief, Defendant was aware of the specific nature of the cyberattack but neglected to reveal that information to Plaintiffs and Class Members, or the relevant states Attorneys General, in any of its public and individual-facing notices. Defendants would have or should have discovered this breach when the PHC data began to be encrypted by Hive on March 19, 2022.

41. A screenshot of HiveLeaks page regarding its alleged theft of PHC data is shown here:



42. Upon information and belief, Plaintiffs' and Class Members' unencrypted information is already for sale on the dark web and may have likely already been purchased by a malicious cybercriminal. According to Hive's posting, the information was disclosed on March 29, 2022. This information is now available

legalscoops.com/partnership-healthplan-of-california-data-breach-possibly-one-of-the-largest-in-health-care/ (last visited June 22, 2022).

[20] *See* Exs. 1,3.

for cybercriminals to misuse and access forever.

43. Unauthorized individuals beyond cybercriminals can easily access the PII and PHI of Plaintiffs and Class Members. For example, this information can fall into the hands of companies that will use the detailed PII and/or PHI for targeted marketing without the approval of Plaintiffs and Class Members, further infringing on their rights.

44. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing their PII and PHI to be exposed.

Defendant Failed to Heed Ransomware Warnings and Take Necessary Precautions

45. PHC has been on notice for almost a year of the potential for a Hive ransomware attack on its systems but did not take sufficient steps to prevent it. Numerous news organizations reported on the threat specifically posed by the Hive group to health service providers following an attack attributed to them on Memorial Health Systems in August 2021.

46. Defendant PHC's negligence in safeguarding the Medical Information, PII and PHI of Plaintiffs and the Class Members was exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data, especially in light of the substantial increase in cyberattacks and/or data breaches in the healthcare and insurance industries preceding the date of this attack.

47. Specifically, as early as July 30, 2021, the U.S. Department of Health and Human Services ("HHS") issued an alert about the Hive group and its potential threat to healthcare organizations.[21]

[21] HHS Cybersecurity Program H3: Section Alert (July 30, 2021), HiveNightmare/SeriousSAM Potential HPH Impact, https://www.hhs.gov/sites/default/files/sector-alert-hive-nightmare-serious-samtlpwhite.pdf (last visited June 21, 2022).

48. In the context of data breaches, healthcare is "by far the most affected industry sector."[22] Further, breaches of cybersecurity in the healthcare industry are particularly devastating, given the frequency of breaches and the fact that healthcare providers maintain highly sensitive and detailed PII and PHI.[23] A Tenable study analyzing publicly disclosed healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in *nearly 93% of the breaches*."[24]

49. Defendant was on further notice regarding the increased risks of inadequate cybersecurity. In February, the cybersecurity arm of the U.S. Department of Health and Human Services ("HHS") issued a warning to hospitals and healthcare systems about a dramatic rise in cyberattacks, including ransomware attacks, urging facilities to shore up their cyber defenses.[25] Indeed, HHS's cybersecurity arm has issued numerous warnings about increased cyberattacks from this very same group, Hive, and urged vigilance with respect to data security.[26]

50. Earlier this year, HHS warned healthcare providers about the increased potential for attacks by Hive, "[c]alling it one of the 'most active ransomware operators in the cybercriminal ecosystem,' the agency said reports have linked Hive to attacks on 355 companies within 100 days of its launch last June — nearly three a day."[27]

---

[22] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches

[23] *See id.*

[24] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (emphasis added).

[25] Rebecca Pifer, *Tenet says 'cybersecurity incident' disrupted hospital operations*, HEALTHCAREDIVE (Apr. 26, 2022), https://www.healthcaredive.com/news/tenet-says-cybersecurity-incident-disrupted-hospital-operations/622692/.

[26] *Id.* (HHS warned healthcare providers about the increased potential for attacks by a ransomware group called Hive, "[c]alling it one of the 'most active ransomware operators in the cybercriminal ecosystem,' the agency said reports have linked Hive to attacks on 355 companies within 100 days of its launch last June — nearly three a day.").

[27] *Id.*

51. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it maintained and stored belonging Plaintiffs and Class Members, causing the exposure and theft of PII and PHI for more than 854,913 individuals.

52. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[28]

53. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.

[28] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for- cisos.pdf/view (last visited June 22, 2022).

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[29]

54. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been

[29] *Id.* at 3-4.

updated with the latest patches. Vulnerable applications and OSs are the target of most ransomwareattacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well asthose you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….
- **Open email attachments with caution**. Be wary of opening emailattachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….
- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing WorkingGroup website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and

email filters—and keep them updated—to reduce malicious network traffic.[30]

55. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
    - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office

[30] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release dateApr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited June 22, 2022).

[Visual Basic for Applications].[31]

56. Given that Defendant was storing the PII and PHI of more than 854,913 individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

57. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII and PHI of approximately 854,913 individuals, including Plaintiffs and Class Members.

Defendant Acquires, Collects and Stores Plaintiffs' and Class Members' PII and PHI.

58. In the course of its regular business operations, Defendant acquired, collected, and stored Plaintiffs' and Class Members' PII and PHI.

59. As a condition of its relationships with Plaintiffs and Class Members, Defendant required that Plaintiffs and Class Members entrust Defendant with highly confidential PII and PHI.

60. By obtaining, collecting, and storing the PII and PHI of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII and PHI from disclosure.

61. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and relied on Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

62. Yet, despite the prevalence of public announcements of these data breach and data security compromises, Defendants failed to take appropriate steps to protect Plaintiffs' and Class Members' PII and PHI from being compromised and

[31] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited June 22, 2022).

failed to timely, properly, and appropriately notify Plaintiffs and Class Members of the true scope and nature of the Data breach.

Securing PII and Preventing Breaches

63. Defendant could have prevented this Data Breach by properly securing and encrypting the PII and PHI of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data, especially years-old data from former enrollees.

64. Defendant's negligence in safeguarding the PII and PHI of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data from ransomware attacks.

65. Indeed, despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiffs and Class Members from being compromised.

66. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[32] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[33]

67. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information and Protected Health Information

[32] 17 C.F.R. § 248.201 (2013).
[33] *Id.*

68. The PII of individuals remains of high value to criminals, as evidenced by the prices criminals will pay for that PII on the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[34] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[35] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[36]

69. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can

[34] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited June 10, 2022).

[35] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited June 10, 2022).

[36] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited June 10, 2022).

cause a lot of problems.[37]

70. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

71. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[38]

72. Further, there is a market for Plaintiffs' and Class Members PHI, and the stolen PII and PHI has inherent value. Sensitive healthcare data can sell for as much as $363 per record according to the Infosec Institute.[39]

73. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies

[37] SOCIAL SECURITY ADMINISTRATION, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 10, 2022).

[38] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited June 10, 2022).

[39] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), available at: https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited June 10, 2022).

purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

74. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[40]

75. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.[41]

76. Based on the foregoing, the information actually or potentially compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information actually or

[40] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News (Feb. 7, 2014) available at: https://khn.org/news/rise-of-indentity-theft/ (last visited June 10, 2022).

[41] FBI Cyber Division, Private Industry Notification, "(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain," Apr. 8, 2014, *available at* http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf (last accessed June 10, 2022).

potentially compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, Social Security number, medical records, and potentially date of birth.

77. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[42]

78. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

79. The PII of Plaintiffs and Class Members was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

80. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from

[42] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited June 10, 2022).

data breaches cannot necessarily rule out all future harm.[43]

81. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiffs and Class Members, including Social Security numbers and/or dates of birth, and of the foreseeable consequences that would occur if PII and PHI were compromised, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members a result.

82. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

83. Defendant was, or should have been, fully aware of the unique type and the significant volume of data stored on and/or shared on its system, amounting to more than 854,913 individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

84. Following the breach and recognizing that Plaintiffs, along with each and every Class Member, are now subject to the present and continuing risk of identity theft and fraud, Defendant offered Plaintiffs and Class Members only twenty-four months of credit monitoring, fraud consultation, and identity theft restoration services through a single provider, TransUnion. The offered services are insufficient to protect Plaintiffs and Class Members from the lifelong implications of having their most private PII and PHI accessed, acquired, exfiltrated, and/or published onto the internet. As another element of damages, Plaintiffs and Class Members seek a sum of money sufficient to provide to Plaintiffs and Class Members identity theft protective services for their respective lifetimes.

85. The injuries to Plaintiffs and Class Members were directly and

[43] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/products/gao-07-737 (last visited June 10, 2022).

proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII and PHI of Plaintiffs and Class Members.

Defendant Failed to Comply with FTC Guidelines

86. Defendant was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

87. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[44]

88. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[45] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

89. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for

[44] Federal Trade Commission, *Start with Security: A Guide for Business, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited June 10, 2022).

[45] Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personal-information.pdf (last visited June 10, 2022).

security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[46]

90. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

91. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C.§ 45.

92. Defendant was at all times fully aware of its obligation to protect the PII and PHI of current and former enrollees because of its status as a healthcare insurer and health plan administrator. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant's Conduct Violates HIPAA

93. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII and PHI like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

94. Defendant's Data Breach resulted from a combination of insufficiencies that indicate Defendant failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Defendant's Data Breach that Defendant either failed to implement, or inadequately

[46] FTC, *Start with Security*, *supra*.

implemented, information security policies or procedures in place to protect Plaintiffs and Class Members' PII and PHI. Second, Defendant's Data Breach could have been prevented if Defendant implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PII and PHI when it was no longer necessary and/or had honored its obligations to its patients.

95. Defendant's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not

permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

i. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 CFR 164.306(a)(94);

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502,et seq.; and

k. Retaining information past a recognized purpose and not deleting it.

96. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[47]

97. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Plaintiffs and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the protected health information and other PII of Plaintiffs and Class Members; and without the supervision of the Court via injunctive relief, Plaintiffs' and Class Members' protected health information and other PII remains at risk of subsequent Data Breaches.

Plaintiff Thomas Shriver's Experience

98. Since approximately 1999, Plaintiff Shriver has been enrolled in Medi-Cal health insurance plan. As a condition of receiving health insurance managed by Defendant, Plaintiffs was required to provide his PII and PHI to Defendant to receive health insurance services. As a condition of receiving these services, Plaintiff Shriver was required to provide his sensitive information, including his PII and PHI.

[47] Breach Notification Rule, U.S. DEP'T OF HEALTH & HUMAN SERVICES, *available at* hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited June 10, 2022).

99. Upon information and belief, Plaintiff Shriver's PHI and PII was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

100. On or around June 17, 2022, Plaintiff received a Notice of Data Breach from Defendant.[48]

101. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone and sorting through his unsolicited emails, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

102. Additionally, Plaintiff is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

103. Plaintiff stores any documents containing his PII in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his few online accounts.

104. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiff entrusted to Defendant for the purpose of obtaining healthcare from Defendant, which was actually or potentially compromised in and as a result of the Data Breach.

105. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy. Plaintiffs has also suffered an increase in spam calls, texts, and emails. These spam calls/texts/emails and phishing attempts have become so frequent and incessant that Plaintiffs has considered changing his phone number.

106. Plaintiff is now subject present and continuing risk of fraud, identity theft, and misuse resulting from his PII and PHI, especially his Social Security

[48] The letter appeared in substantially the same form as the Sample Letters provided to the states Attorneys General.

number, in combination with his name, being placed in the hands of unauthorized third parties and possibly criminals. This injury was worsened by Defendant's continuing delay in revealing the true nature of the threat to Plaintiff's PII and PHI.

107. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff James Lee's Experience

108. Since approximately 2015, Plaintiff Lee has been enrolled in Medi-Cal health insurance plan. As a condition of receiving health insurance managed by Defendant, Plaintiffs was required to provide his PII and PHI to Defendant to receive health insurance services. As a condition of receiving these services, Plaintiff Lee was required to provide his sensitive information, including his PII and PHI.

109. Upon information and belief, Plaintiff Lee's PHI and PII was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

110. On or around June 17, 2022, Plaintiff received a Notice of Data Breach from Defendant.[49]

111. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone and sorting through his unsolicited emails, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

112. Additionally, Plaintiff is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

[49] The letter appeared in substantially the same form as the Sample Letters provided to the states Attorneys General.

113. Plaintiff stores any documents containing his PII in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his few online accounts.

114. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiff entrusted to Defendant for the purpose of obtaining healthcare from Defendant, which was actually or potentially compromised in and as a result of the Data Breach.

115. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy. Plaintiff has also suffered an increase in spam calls, texts, and emails. These spam calls/texts/emails and phishing attempts have become so frequent and incessant that Plaintiff has considered changing his phone number.

116. Plaintiff is now subject present and continuing risk of fraud, identity theft, and misuse resulting from his PII and PHI, especially his Social Security number, in combination with his name, being placed in the hands of unauthorized third parties and possibly criminals. This injury was worsened by Defendant's continuing delay in revealing the true nature of the threat to Plaintiff's PII and PHI.

117. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

118. Plaintiffs seek relief on behalf of themselves and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. Rule 23(a), (b)(2), (b)(3) and (c)(4), Plaintiffs seek certification of a Nationwide Class defined as follows:

> **All individuals residing in the United States whose PII was actually or potentially compromised during the data event PHC identified on or about March 19, 2022**

(the "Nationwide Class").

119. In the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs asserts claims on behalf of a separate subclass, defined as follows:

> **All individuals residing in California whose PII was actually or potentially compromised during the data event PHC identified on or about March 19, 2022 (the "California Class").**

120. Excluded from the Nationwide Class and the California Class (collectively the "Classes") are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members and staff.

121. Plaintiffs reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

122. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

123. **Risk of Inconsistent or Varying Adjudications. Fed. R. Civ. P. 23(b)(1).** As the proposed Class Members include many individuals, there is significant risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for the Defendant. For example, injunctive relief may be entered in multiple cases, but the ordered relief may vary, causing Defendant to have to choose between differing means of upgrading their data security practices and choosing the court order with which they will comply. Class action status is also warranted because prosecution of separate actions by the members of the Class would create a risk of adjudications

with respect to individual members of the Class that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

124. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are believed to be so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of individuals affected in the Data Breach is unknown, upon information and belief, it is over 854,913.

125. **Commonality and Predominance. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include:

a. Whether Defendant had a duty to protect its enrollees' sensitive PII and PHI;
b. Whether Defendant knew or should have known of the susceptibility of its systems to a data breach;
c. Whether Defendant's security measures to protect its systems were reasonable in light of best practices recommended by data security experts;
d. Whether Defendant was negligent in failing to implement reasonable and adequate security procedures and practices;
e. Whether Defendant's failure to implement adequate data security measures allowed the breach of its data systems to occur;
f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the unlawful exposure of the Plaintiffs' and Class Members' PII and PHI;
g. Whether Plaintiffs and Class Members were injured and suffered

damages or other losses because of Defendant's failure to reasonably protect their systems and data network; and

h. Whether Plaintiffs and Class members are entitled to relief.

126. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiffs' claims are typical of those of other Class Members. Plaintiffs' damages and injuries are akin to other Class Members, and Plaintiffs seek relief consistent with the relief sought by the Class.

127. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs is an adequate representative of the Class because he is a member of the Class he seek to represent; is committed to pursuing this matter against Defendant to obtain relief for the Class; and has no conflicts of interest with the Class. Moreover, Plaintiffs' attorneys are competent and experienced in litigating class actions, including privacy litigation of this kind. Plaintiffs intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

128. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to an individual Plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Defendant, and thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

129. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through their uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

130. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII and PHI;
b. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;
c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
d. Whether Defendant failed to take commercially reasonable steps to safeguard PII and PHI;
e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach;
f. Whether Defendant failed to comply with its statutory and regulatory obligations; and,
g. Whether Plaintiffs and the proposed Class are entitled to compensation as a result of Defendant's actions.

131. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names of those affected by the Data Breach. Using this information, Class Members can be identified and ascertained for the purpose of providing notice.

VI. FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

132. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 131.

133. Plaintiffs and the Nationwide Class provided and entrusted Defendant with certain PII and PHI, including, without limitation, name, Social Security number, date of birth, Driver's License number (if provided), Tribal ID number (if provided), medical record number, treatment, diagnosis, prescription and other medical information, health insurance information, member portal username and password, email address, and address.

134. Plaintiffs and the Nationwide Class entrusted their PII and PHI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third parties.

135. Defendant has full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiffs and the Nationwide Class could and would suffer if the PII and PHI were wrongfully disclosed.

136. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII and PHI of Plaintiffs and the Nationwide Class involved an unreasonable risk of harm to Plaintiffs and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

137. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII and PHI of Plaintiffs and the Nationwide Class in Defendant's possession was adequately secured and protected.

138. Defendant also had a duty to exercise appropriate clearinghouse

practices to remove PII and PHI it was no longer required to retain pursuant to regulations, including that of former customers or patients.

139. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiffs and the Nationwide Class.

140. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Nationwide Class. That special relationship arose because Plaintiffs and the Nationwide Class entrusted Defendant with their confidential PII and PHI, a necessary part of their relationships with Defendant.

141. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Nationwide Class.

142. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices and Defendant's previous data breach, just last year.

143. Plaintiffs and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiffs and the Nationwide Class, the critical importance of providing adequate security of that PII and PHI, and the necessity for encrypting PII and PHI stored on Defendant's systems.

144. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiffs and the Nationwide Class, including basic encryption techniques freely available to Defendant.

145. Plaintiffs and the Nationwide Class had no ability to protect their PII and PHI that was in, and possibly remains in, Defendant's possession.

146. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Nationwide Class as a result of the Data Breach.

147. Defendant had and continues to have a duty to adequately disclose that the PII and PHI of Plaintiffs and the Nationwide Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Nationwide Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third parties.

148. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiffs and the Nationwide Class.

149. Defendant has admitted that the PII and PHI of Plaintiffs and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

150. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiffs and the Nationwide Class during the time the PII and PHI was within Defendant's possession or control.

151. Defendant improperly and inadequately safeguarded the PII and PHI of Plaintiffs and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

152. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiffs and the Nationwide Class in the face of increased risk of theft.

153. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Nationwide Class by failing to have appropriate

procedures in place to detect and prevent dissemination of their PII and PHI.

154. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII and PHI it was no longer required to retain pursuant to regulations.

155. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Nationwide Class the existence and scope of the Data Breach.

156. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the PII and PHI of Plaintiffs and the Nationwide Class would not have been actually or potentially compromised.

157. There is a close causal connection between Defendant's failure to implement security measures to protect the PII and PHI of Plaintiffs and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The PII and PHI of Plaintiffs and the Nationwide Class was actually or potentially compromised as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures.

158. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII and PHI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

159. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Nationwide Class.

160. Defendant's violation of Section 5 of the FTC Act constitutes

negligence *per se*.

161. Plaintiffs and the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

162. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Nationwide Class.

163. Defendant's violation of HIPAA also independently constitutes negligence *per se*.

164. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of enrollees ' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

165. Plaintiffs and the Nationwide Class are within the class of persons that HIPAA privacy laws were intended to protect.

166. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

167. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate

the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiffs and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

168. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

169. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI in its continued possession.

170. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

VII. SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

171. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 131.

172. Defendant required Plaintiffs and the Nationwide Class to provide and entrust their PII and PHI, including, without limitation, name, Social Security number, date of birth, Driver's License number (if provided), Tribal ID number (if provided), medical record number, treatment, diagnosis, prescription and other medical information, health insurance information, member portal username and password, email address, and address as a condition of obtaining medical care from Defendant.

173. Defendant's Privacy Policy states that Defendant has "policies and procedures for preserving the confidentiality of medical records is available and will be furnished to you upon request."[50]

174. Further, the Privacy Policy lists situations under which PHC may disclose PHI and PII of its enrollees without written authorization – none of which are applicable here.[51]

175. In addition, the Privacy Policy explicitly states:

> OTHER THAN WHAT IS STATED ABOVE, PHC WILL NOT DISCLOSE YOUR HEALTH INFORMATION OTHER THAN WITH YOUR WRITTEN AUTHORIZATION. IF YOU OR YOUR REPRESENTATIVE AUTHORIZES PHC TO USE OR DISCLOSE YOUR HEALTH INFORMATION, YOU MAY REVOKE THAT AUTHORIZATION IN WRITING AT ANY TIME.[52]

176. Defendant solicited and invited Plaintiffs and Class Members to provide their PII and PHI as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PII and PHI to Defendant.

177. As a condition of obtaining care from Defendant, Plaintiffs and the Nationwide Class provided and entrusted their personal information. In so doing,

[50] Ex. 2, at 93.
[51] *Id.*
[52] *Id.*, at 97.

Plaintiffs the Nationwide Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Nationwide Class if their data had been breached and compromised or stolen.

178. A meeting of the minds occurred when Plaintiffs and the Class Members agreed to, and did, provide their PII and PHI to Defendant, in exchange for, amongst other things, the protection of their PII and PHI.

179. Plaintiffs and the Nationwide Class fully performed their obligations under the implied contracts with Defendant.

180. Defendant breached the implied contracts it made with Plaintiffs and the Nationwide Class by failing to safeguard and protect their personal and financial information and by failing to provide timely and accurate notice to them that personal and financial information was compromised as a result of the data breach.

181. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Nationwide Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

182. As a result of Defendant's breach of implied contract, Plaintiffs and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

VIII. THIRD CAUSE OF ACTION

Invasion of Privacy
(On Behalf of Plaintiffs and the Nationwide Class)

183. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 131.

184. Plaintiffs and the Nationwide Class had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

185. Defendant owed a duty to its current and former enrollees, including Plaintiffs and the Nationwide Class, to keep their PII and PHI contained as a part thereof, confidential.

186. Defendant failed to protect and allowed to be accessed, viewed, or released to unknown and unauthorized third parties the PII and PHI of Plaintiffs and the Nationwide Class.

187. Defendant allowed unauthorized and unknown third parties to access, examine, exfiltrate, and/or publish the PII and PHI of Plaintiffs and the Nationwide Class, by way of Defendant's failure to protect the PII and PHI.

188. The unauthorized release to, custody of, and/or examination by unauthorized third parties of the PII and PHI of Plaintiffs and the Nationwide Class is highly offensive to a reasonable person.

189. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Nationwide Class disclosed their PII and PHI to Defendant as part of Plaintiffs' and the Nationwide Class's relationships with Defendant, but privately with an intention that the PII and PHI would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Nationwide Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

190. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs' and the Nationwide Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind

that would be highly offensive to a reasonable person.

191. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

192. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Nationwide Class.

193. As a proximate result of the above acts and omissions of Defendant, the PII and PHI of Plaintiffs and the Nationwide Class was accessed by to third parties without authorization, causing Plaintiffs and the Nationwide Class to suffer damages.

194. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Nationwide Class in that the PII and PHI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Nationwide Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Nationwide Class.

IX. FOURTH CAUSE OF ACTION
Violations of California's Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq*.
(On behalf of Plaintiffs and the California Class)

195. Plaintiffs and the California Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 131.

196. Defendant is a "provider of health care" as defined in Cal. Civ. Code § 56.05(a), as Defendant PHC is a "health care service plan" as defined by Cal. Civ. Code section 56.05(f) and is therefore subject to the requirements of the CMIA.[53]

197. Defendant created, maintained, preserved, and stored Plaintiffs' and the California Class's "medical information," as defined under Cal. Civ. Code § 56.05(j), which was subject to the Data Breach.

198. Plaintiffs and the California Class are "patients" as defined by Cal. Civ. Code § 56.05(k).

199. As a provider of health care, Defendant owed a duty to preserve the confidentiality of Plaintiffs' and members of the California Class's medical information and to not allow Plaintiffs' and members of the California Class's medical information to be released and viewed by unauthorized persons.

200. Defendant breached its duty owed to Plaintiffs and the members of the California Class by failing to implement fair, reasonable, or adequate computer systems and data security policies to safeguard Plaintiffs' and California Class Members' medical information, and by allowing that PHI to be released and viewed by unauthorized persons.

201. In violation of the first sentence of Cal. Civ. Code § 65.101(a), Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of medical information (including Plaintiffs' and California Class Members' PHI (including medical information)) in a manner that failed to preserve and breached the confidentiality of the information contained therein. The resulting unauthorized access and potential acquisition of Plaintiffs' and California Class Members' PHI to unauthorized hackers during the Data Breach was an affirmative communicative act in violation of violation of Cal. Civ. Code § 56.101(a). Plaintiffs' and California

[53] At all relevant times, Defendant was healthcare provider for the purposes of this cause of action because it had the "purpose of maintaining medical information . . . in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or his information, or for the diagnosis or treatment of the individual." Cal. Civ. Code § 56.06(a).

Class Members' PHI was viewed by the unauthorized hackers as a direct and proximate result of Defendant's violation of Cal. Civ. Code § 56.101(a).

202. In violation of the second sentence of Cal. Civ. Code § 56.101(a), Defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of medical information (including Plaintiffs' and California Class Members' PHI (including medical information)). The resulting unauthorized access and potential acquisition of Plaintiffs' and California Class Members' PHI to unauthorized hackers during the Data Breach was an affirmative communicative act in violation of violation of Cal. Civ. Code § 56.101(a). Plaintiffs' and California Class Members' PHI was viewed by the unauthorized hackers as a direct and proximate result of Defendant's violation of Cal. Civ. Code § 56.101(a).

203. Plaintiffs' and California Class Members' PHI that was subject to the Data Breach included "electronic medical records" or "electronic health records" as referenced by Cal. Civ. Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

204. In violation of Cal. Civ. Code § 56.101(b)(1)(A), Defendant's electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information (including Plaintiffs' and California Class Members' PHI). The resulting unauthorized access and potential acquisition of Plaintiffs' and California Class Members' PHI to and/or by unauthorized hackers during the Data Breach was an affirmative communicative act in violation of violation of Cal. Civ. Code § 56.101(b)(1)(A). Plaintiffs' and California Class Members' PHI was viewed by the unauthorized hackers as a direct and proximate result of Defendant's violation of Cal. Civ. Code § 56.101(b)(1)(A).

205. In violation of Cal. Civ. Code § 56.101(b)(1)(B), Defendant's electronic health record system or electronic medical record system failed to automatically record and preserve any actual or potential change or deletion of any electronically stored medical information (including Plaintiffs' and California Class Members' PHI).

206. In violation of Cal. Civ. Code § 56.101(b)(1)(B), Defendant's electronic health record system or electronic medical record system failed to record the identity of persons who actually or potentially accessed and changed medical information (including Plaintiffs' and California Class Members' PHI), failed to record the date and time medical information was accessed (including Plaintiffs' and California Class Members' PHI) and failed to record any actual or potential changes that were made to medical information (including Plaintiffs' and California Class Members' PHI).

207. In violation of Cal. Civ. Code § 56.36(b), Defendant negligently released confidential information or records concerning Plaintiffs' and California Class Members' PHI. This negligent release of Plaintiffs' and California Class Members' PHI to unauthorized hackers during the Data Breach was an affirmative communicative act in violation of Cal. Civ. Code § 56.36(b). Plaintiffs' and California Class Members' PHI was viewed by the unauthorized hackers as a direct and proximate result of Defendant's violation of Cal. Civ. Code § 56.36(b).

208. In violation of Cal. Civ. Code § 56.10(e), Defendant disclosed Plaintiffs' and California Class Members' PHI to persons or entities not engaged in providing direct health care services to Plaintiffs' or California Class Members or their providers of health care or health care service plans or insurers or self-insured employers.

209. The foregoing violations of CMIA resulted from Defendant's affirmative actions, and Defendant knew or should have known it had inadequate computer systems and data security practices to safeguard such information. Defendant knew or should have known of the risks inherent in collecting and storing the protected medical information of Plaintiffs and members of the California Class.

210. The injury and harm Plaintiffs and members of the California Class suffered was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and its breach would cause Plaintiffs and members of the California Class to suffer the

foreseeable harms associated with the exposure of their PHI, including medical information.

211. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and members of the California Class are now subject to the present and continuing risk of identity theft and other harms.

212. Pursuant to Cal. Civ. Code §§ 56.35 and 56.36, Plaintiffs and each member of the California Class seek relief including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorney fees, expenses, and costs. A recovery of nominal damages does not require that Plaintiffs or members of the California Class have suffered or have been threatened with actual damages.

213. As a direct and proximate result of Defendant's violation of Cal. Civ. Code § 56, *et seq*., Plaintiffs and members of the California Class are now subject to the present and continuing risk of identity theft and other harms.

214. As a direct and proximate result of Defendant's violation of Cal. Civ. Code § 56, *et seq*., Plaintiffs and members of the California Class have suffered injury and are entitled to damages in an amount to be proven at trial.

215. Plaintiffs and members of the California Class suffered a privacy injury by having their sensitive medical information disclosed, irrespective of whether they subsequently suffered identity fraud or incurred any mitigation damages. PHI has been recognized as private sensitive information in common law and federal and state statutory schemes and the disclosure of such information resulted in cognizable injury to Plaintiffs and members of the California Class.

X. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the California Class, and appointing Plaintiffs and their Counsel to represent each such

Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the PII and PHI of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to

conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and

periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, nominal, and statutory damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: June 23, 2022

Respectfully Submitted,

By: */s/ Michael F. Ram*
Michael F. Ram

MICHAEL F. RAM (SBN 104805)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
Telephone: (415) 358-6913
Facsimile: (415) 358-6923
mram@ForThePeople.com

JOHN YANCHUNIS
(*Pro Hac Vice application forthcoming*)
PATRICK BARTHLE
(*Pro Hac Vice application forthcoming*)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 559-4908
Facsimile: (813) 222-4795
jyanchunis@ForThePeople.com
pbarthle@ForThePeople.com

Attorneys for Plaintiffs and the Putative Class